

Junos[®] OS Release 12.1X46 Feature Guide

Junos OS Release 12.1X46-D15
6 March 2014
Revision 1

This feature guide accompanies Junos OS Release 12.1X46-D15. This guide contains detailed information about features introduced in Junos OS Release 12.1X46-D15 that are summarized in the Release Notes.

Contents

New Features in Junos OS Release 12.1X46-D15	2
IP Monitoring	2
Next-Hop Functionality	2
Routing Protocols	6
OSPF Nonbroadcast Multiaccess and Point-to-Multipoint Network Support	6
Documentation Feedback	11
Requesting Technical Support	11
Self-Help Online Tools and Resources	11
Opening a Case with JTAC	12
Revision History	12

New Features in Junos OS Release 12.1X46-D15

Junos OS Release 12.1X46-D15 introduces the following features:

- [IP Monitoring on page 2](#)
- [Routing Protocols on page 6](#)

IP Monitoring

This topic includes the following section:

- [Next-Hop Functionality on page 2](#)

Next-Hop Functionality

- `show services ip-monitoring status`

show services ip-monitoring status

Syntax	show services ip-monitoring status
Release Information	Command modified in Junos OS Release 11.4 R2. Next-hop functionality added in Junos OS Release 12.1X46-D15.
Description	Display a brief summary of IP monitoring status along with the current state for a given policy.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>IP Monitoring Feature Guide for Security Devices</i> • <i>show services rpm probe-results (View)</i>
List of Sample Output	show services ip-monitoring status on page 4 show services ip-monitoring status on page 4 show services ip-monitoring status on page 5 show services ip-monitoring status on page 5 show services ip-monitoring status on page 5
Output Fields	Table 1 on page 3 lists the output fields for the show services ip-monitoring status command. Output fields are listed in the approximate order in which they appear.

Table 1: show services ip-monitoring status Output Fields

Field Name	Field Description
Policy	Name of the policy configured.
Probe Name	Name of the probe configured.
Address	Displays the configured target address.
Status	Displays the status of the probe on the target address. If the status is PASS, then the target address is reached.
Route-Action	Displays route injection information configured for the policy and its failover status.
Route-Instance	Displays the routing instance of the route to be injected during failover.
Route	Routing address of the route to be injected during failover.
Next-Hop	Specifies the next-hop address of the route to be injected during failover. P2P interfaces only.
State	Displays the state of the route injection action. If the state is APPLIED, then the ip-monitoring policy is in failover state.

Table 1: show services ip-monitoring status Output Fields (*continued*)

Field Name	Field Description
Interface Action	Displays the interface action type as enable or disable.
Policy Action	Displays the policy action type as enable or disable.
Admin State	Displays the current admin state of the interface.
Action Status	Displays the current action status of the interface.

Sample Output

show services ip-monitoring status

```
user@host> show services ip-monitoring status
```

```
Policy - policy1 (Non-preemptive. Status: FAIL)
```

```
RPM Probes:
```

Probe name	Test Name	Address	Status
probe_a	a1	15.1.1.10	FAIL
probe_a	a2	200.1.1.1	FAIL

```
Route-Action:
```

route-instance	route	next-hop	State
inet.0	200.1.1.0	150.1.1.1	APPLIED

```
Interface-Action:
```

interface	policy action	admin state	action status
fe-0/0/5.2	Enable	UP	FAILOVER
fe-0/0/5.4	Disable	DOWN	FAILOVER
t1-1/0/0	Enable	UP	FAILOVER
d10	Enable	UP	FAILOVER
ge-0/0/1	Enable	UP	FAILOVER

Sample Output

show services ip-monitoring status

In this example, the policy is in the failback state, and the no-preempt option is not configured.

```
user@host> show services ip-monitoring status
```

```
Policy - policy1 (Status: PASS)
```

```
RPM Probes:
```

Probe name	Test Name	Address	Status
probe1	a1	99.1.1.2	PASS

```
Route-Action:
```

route-instance	route	next-hop	state
inet.0	99.1.1.0	12.12.12.2	NOT-APPLIED

```
Interface-Action:
```

interface	policy action	admin state	action status
at-2/0/0	Enable	DOWN	MARKED-DOWN
ge-0/0/2.2	Enable	DOWN	MARKED-DOWN
ge-0/0/2.3	Enable	DOWN	MARKED-DOWN

Sample Output

show services ip-monitoring status

In this example, the policy is in the failover state, and the primary is restored. The no-preempt option is configured.

```
user@host> show services ip-monitoring status
```

Policy - policy1 (Non-preemptive. Status: FAILOVER-NO-PREEMPT)

RPM Probes:

Probe name	Test Name	Address	Status
probe1	a1	99.1.1.2	PASS

Route-Action:

route-instance	route	next-hop	state
inet.0	99.1.1.0	12.12.12.2	APPLIED

Interface-Action:

interface	policy action	admin state	action status
at-2/0/0	Enable	UP	FAILOVER
ge-0/0/2.2	Enable	UP	FAILOVER
ge-0/0/2.3	Enable	UP	FAILOVER

Sample Output

show services ip-monitoring status

When the probe succeeds and the policy is not applied, the output is as follows:

```
user@host> show services ip-monitoring status
```

Policy payment (Status: PASS)

RPM Probes:

Probe name	Test Name	Address	Status
Probe-Payment-Server	paysvr	9.9.9.2	PASS

Route-Action:

route-instance	route	next-hop	state
inet.0	9.9.9.0/24	e1-6/0/0.0	NOT-APPLIED

Sample Output

show services ip-monitoring status

When the probe fails and the policy is applied, the output is as follows:

```
user@host> show services ip-monitoring status
```

Policy payment (Status: FAIL)

RPM Probes:

Probe name	Test Name	Address	Status
Probe-Payment-Server	paysvr	9.9.9.2	FAIL

Route-Action:			
route-instance	route	next-hop	state
inet.0	9.9.9.0/24	e1-6/0/0.0	APPLIED

Routing Protocols

This topic includes the following section:

- [OSPF Nonbroadcast Multiaccess and Point-to-Multipoint Network Support on page 6](#)

OSPF Nonbroadcast Multiaccess and Point-to-Multipoint Network Support

- [Example: Configuring an OSPF Interface on a Nonbroadcast Multiaccess Network on page 6](#)
- [Example: Configuring an OSPF Interface on a Point-to-Multipoint Network on page 9](#)

Example: Configuring an OSPF Interface on a Nonbroadcast Multiaccess Network

This example shows how to configure an OSPFv2 interface on a nonbroadcast multiaccess (NBMA) network on high-end SRX Series devices.

- [Requirements on page 6](#)
- [Overview on page 6](#)
- [Configuration on page 7](#)
- [Verification on page 8](#)

Requirements

Before you begin:

- Configure the router identifiers for the devices in your OSPF network. See *Example: Configuring an OSPF Router Identifier*.
- Control OSPF designated router election. See *Example: Controlling OSPF Designated Router Election*.
- Configure a multiarea OSPF network. See *Example: Configuring a Multiarea OSPF Network*.

Overview

When you configure OSPFv2 on an NBMA network, you can use nonbroadcast mode to interoperate with other equipment. Because there is no autodiscovery mechanism, you must configure each neighbor.

Nonbroadcast mode treats the NBMA network as a partially connected LAN, electing designated and backup designated routers. All routing devices must have a direct connection to both the designated and backup designated routers; otherwise, unpredictable results can occur.

When you configure the interface, specify either the IP address or the interface name. Using both the IP address and the interface name produces an invalid configuration. For

nonbroadcast interfaces, specify the IP address of the nonbroadcast interface as the interface name.

In this example, you configure the Ethernet interface xe-2/0/0.0 as an OSPFv2 interface in OSPF area 0.0.0.1 and specify the following settings:

- **interface-type nbma**—Sets the interface to run in NBMA mode. You must explicitly configure the interface to run in NBMA mode.
- **neighbor address <eligible>**—Specifies the IP address of the neighboring device as 192.0.1.2. If you want the neighbor to be a designated router, include the **eligible** keyword.



NOTE: OSPF routing devices normally discover their neighbors dynamically by listening to the broadcast or multicast hello packets on the network. Because an NBMA network does not support broadcast (or multicast), the device cannot discover its neighbors dynamically, so you must configure all the neighbors statically. To configure multiple neighbors, include multiple **neighbor** statements.

- **hello-interval**—Specifies the length of time, in seconds, before the device sends hello packets out of the interface before it establishes adjacency with a neighbor.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter **commit** from configuration mode.

```
[edit]
set interfaces xe-2/0/0 unit 0 family inet address 192.0.2.1/24
set protocols ospf area 0.0.0.1 interface xe-2/0/0.0 interface-type nbma
set protocols ospf area 0.0.0.1 interface xe-2/0/0.0 neighbor 192.0.2.2 eligible
set protocols ospf area 0.0.0.1 interface xe-2/0/0.0 hello-interval 130
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure an OSPFv2 interface on an NBMA network:

1. Configure the interface.

```
[edit]
user@host# set interfaces xe-2/0/0 unit 0 family inet address 192.0.2.1/24
```
2. Create an OSPF area.

```
[edit]
user@host# edit protocols ospf area 0.0.0.1
```
3. Assign the interface to the area.

In this example, include the **eligible** keyword to allow the neighbor to be a designated router.

```
[edit protocols ospf area 0.0.0.1 ]
user@host# set interface xe-2/0/0.0 interface-type nbma neighbor 192.0.2.2 eligible
```

4. Configure the hello interval.

```
[edit protocols ospf area 0.0.0.1 ]
user@host# set interface xe-2/0/0.0 hello-interval 130
```

Results

From configuration mode, confirm your configuration by entering the **show interfaces** and the **show protocols ospf** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show interfaces
xe-2/0/0 {
  unit 0 {
    family inet {
      address 192.0.2.1/24;
    }
  }
}

user@host# show protocols ospf
area 0.0.0.1 {
  interface xe-2/0/0.0 {
    interface-type nbma;
    neighbor 192.0.2.2 eligible;
    hello-interval 130;
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the OSPF Interface

Purpose Verify the interface configuration by confirming that the **Type** field displays NBMA.

Action From operational mode, enter the **show ospf interface detail** command.

Related Documentation

- *OSPF Configuration Overview*
- *About OSPF Interfaces*
- *OSPF Timers Overview*

Example: Configuring an OSPF Interface on a Point-to-Multipoint Network

This example shows how to configure an OSPF interface on a point-to-multipoint network high-end SRX Series devices.

- [Requirements on page 9](#)
- [Overview on page 9](#)
- [Configuration on page 9](#)
- [Verification on page 10](#)

Requirements

Before you begin:

- Configure the router identifiers for the devices in your OSPF network. See *Example: Configuring an OSPF Router Identifier*.
- Control OSPF designated router election. See *Example: Controlling OSPF Designated Router Election*
- Configure a multiarea OSPF network. See *Example: Configuring a Multiarea OSPF Network*.

Overview

When you configure OSPFv2 on a nonbroadcast multiaccess (NBMA) network, such as a multipoint Asynchronous Transfer Mode (ATM) or Frame Relay, OSPFv2 operates by default in point-to-multipoint mode. In this mode, OSPFv2 treats the network as a set of point-to-point links. Because there is no autodiscovery mechanism, you must configure each neighbor.

When you configure the interface, specify either the IP address or the interface name. Using both the IP address and the interface name produces an invalid configuration.

In this example, you configure the Ethernet interface xe-2/0/0.0 as an OSPFv2 interface in OSPF area 0.0.0.1 and specify 192.0.2.1 as the neighbor's IP address.

Configuration**CLI Quick
Configuration**

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the [edit] hierarchy level, and then enter **commit** from configuration mode.

```
[edit]
set interfaces xe-2/0/0 unit 0 family inet address 192.0.2.2/24
set protocols ospf area 0.0.0.1 interface xe-2/0/0 neighbor 192.0.2.1
set protocols ospf area 0.0.0.1 interface xe-2/0/0 interface-type p2mp
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure an OSPFv2 interface on a point-to-multipoint network:

1. Configure the interface.

```
[edit]
user@host# set interfaces xe-2/0/0 unit 0 family inet address 192.0.2.2/24
```

2. Create an OSPF area.

```
[edit]
user@host# edit protocols ospf area 0.0.0.1
```

3. Assign the interface to the area and specify the neighbor.

```
[edit protocols ospf area 0.0.0.1]
user@host# set interface xe-2/0/0 neighbor 192.0.2.1
```

To configure multiple neighbors, include a **neighbor** statement for each neighbor.

4. Specify the interface type as **p2mp**.

```
[edit protocols ospf area 0.0.0.1]
user@host# set interface xe-2/0/0 interface-type p2mp
```

Results

From Configuration mode, confirm your configuration by entering the **show interfaces** and the **show protocols ospf** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show interfaces
xe-2/0/0 {
  unit 0 {
    family inet {
      address 192.0.2.2/24;
    }
  }
}

user@host# show protocols ospf
area 0.0.0.1 {
  interface xe-2/0/0 {
    interface-type p2mp;
    neighbor 192.0.2.1;
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Verifying the OSPF Interface

Purpose Verify the interface configuration by confirming that the **Type** field displays P2MP.

Action From operational mode, enter the **show ospf interface detail** command.

Related Documentation

- *OSPF Configuration Overview*
- *About OSPF Interfaces*

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>

- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

Revision History

6 March 2014—Revision 1, Junos OS Release 12.1X46-D15 Feature Guide

Copyright © 2014, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.